UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/578,177	12/15/2006	Makoto Saito	290398US2PCT	5196

22850 7590 04/23/2010

OBLON, SPIVAK, MCCLELLAND MAIER & NEUSTADT, L.L.P.
1940 DUKE STREET
ALEXANDRIA, VA 22314

EXAMINER	
MOORTHY, ARAVIND K	

ART UNIT	PAPER NUMBER
2431	

NOTIFICATION DATE	DELIVERY MODE
04/23/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patentdocket@oblon.com
oblonpat@oblon.com
jgardner@oblon.com

Office Action Summary	Application No.	Applicant(s)	
	10/578,177	SAITO ET AL.	
	Examiner	Art Unit	
	Aravind K. Moorthy	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 October 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-43* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-43* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *04 May 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This is in response to the communications filed on 5 October 2007.

2. Claims 1-43 are pending in the application.

3. Claims 1-43 have been rejected.

Information Disclosure Statement

4. The examiner has considered the information disclosure statement (IDS) filed on 14 July 2006, 18 April 2007, 11 May 2007 and 5 October 2007.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

5. Claims 3-24, 27-38, 42 and 43 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Independent claim 3 is directed towards a session management apparatus for establishing an encrypted communication channel between a first apparatus and a second apparatus. However, after a review of the applicant's specification, the examiner has found no support for the first and second apparatus being hardware. Since there is no hardware, this renders the claims non-statutory.

Independent claim 15 is directed towards an apparatus that establishes an encrypted communication channel to a second apparatus by using a session management apparatus. However, after a review of the applicant's specification, the examiner has found no support for the second apparatus and the session management apparatus being hardware. Since there is no hardware, this renders the claims non-statutory.

Independent claim 19 is directed towards a computer program for causing a computer to function as a session management apparatus that is used for establishing an encrypted communication channel between a first apparatus and a second apparatus that are connected to a communication network. Since a computer program is non-statutory material, this renders the claim non-statutory.

Independent claim 22 is directed towards a computer program for causing a computer to function as an apparatus that establishes an encrypted communication channel to a second apparatus by using a session management apparatus. Since a computer program is non-statutory material, this renders the claim non-statutory.

Independent claim 27 is directed towards a public-key management apparatus for managing public-keys used for establishing an encrypted communication channel between a first apparatus and a second apparatus. However, after a review of the applicant's specification, the examiner has found no support for the first and second apparatus being hardware. Since there is no hardware, this renders the claims non-statutory.

Independent claim 30 is directed towards a public-key management apparatus for managing public-keys used for establishing an encrypted communication channel between a first apparatus and a second apparatus. However, after a review of the applicant's specification, the examiner has found no support for the first and second apparatus being hardware. Since there is no hardware, this renders the claims non-statutory.

Independent claim 33 is directed towards a computer program for causing a computer to function as a public-key management apparatus for managing public-keys. Since a computer program is non-statutory material, this renders the claim non-statutory.

Independent claim 34 is directed towards a computer program for causing a computer to function as a public-key management apparatus for managing public-keys used for establishing an encrypted communication channel between a first apparatus and a second apparatus. Since a computer program is non-statutory material, this renders the claim non-statutory.

Independent claim 35 is directed towards a session management apparatus that can connect to a first apparatus and a second apparatus over a network. However, after a review of the applicant's specification, the examiner has found no support for the first and second apparatus being hardware. Since there is no hardware, this renders the claims non-statutory.

Independent claim 37 is directed towards a session management apparatus that can connect to a first apparatus and a second apparatus over a network. However, after a review of the applicant's specification, the examiner has found no support for the first and second apparatus being hardware. Since there is no hardware, this renders the claims non-statutory.

Independent claim 42 is directed towards a computer program for causing a computer to function as a session management apparatus that can connect to a first apparatus and a second apparatus over a network. Since a computer program is non-statutory material, this renders the claim non-statutory.

Independent claim 43 is directed towards a computer program for causing a computer to function as a session management apparatus that can connect to a first apparatus and a second apparatus over a network. Since a computer program is non-statutory material, this renders the claim non-statutory.

Any claims not directly addressed are rejected on the virtue of their dependency.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 1-43 are rejected under 35 U.S.C. 102(e) as being anticipated by Birger et al US 2009/0006850 A1 (hereinafter Birger).

As to claim 1, Birger discloses a method for establishing an encrypted communication channel between a first apparatus and a second apparatus by using a session management apparatus, comprising the steps of:

establishing a first encrypted communication channel between the session management apparatus (i.e. ICL relay) and the first apparatus by performing mutual authentication between the session management apparatus and the first apparatus (i.e. The ICL helps to ensure that devices and users are authenticated an authorized and that communication messages are encrypted to maintain their integrity) [0064];

establishing a second encrypted communication channel between the session management apparatus and the second apparatus by performing mutual authentication between the session management apparatus and the second apparatus (i.e. The registration process involves a mutual authentication between the endpoint and the authentication service.) [0209]; and

exchanging key information between the first apparatus and the second apparatus via the first encrypted communication channel and the second encrypted communication channel so as to establish an encrypted communication channel between the first apparatus and the second apparatus (i.e. The exchange of session key information.) [0211].

As to claim 2, Birger discloses a method for establishing an encrypted communication channel between a first apparatus and a second apparatus by using a session management apparatus, wherein:

the session management apparatus (i.e. ICL relay and the first apparatus exchange key information for encrypted communication (i.e. The exchange of session key information.) [0211], and performs mutual authentication so as to establish a first encrypted communication channel between the session management apparatus and the first apparatus (i.e. The registration process involves a mutual authentication between the endpoint and the authentication service.) [0209];

the session management apparatus and the second apparatus exchange key information for encrypted communication, and performs mutual authentication so as to establish a second encrypted communication channel between the session management apparatus and the second apparatus (i.e. The exchange of session key information) [0214];

the first apparatus sends, to the session management apparatus via the first encrypted communication channel, a connection request message destined for the

second apparatus including key information used for encrypted communication between the first apparatus and the second apparatus, and the session management apparatus sends the connection request message to the second apparatus via the second encrypted communication channel (i.e. Figure 9 illustrates authentication and establishing a connection) [0222-0223]; and

the second apparatus sends, to the session management apparatus via the second encrypted communication channel, a response message including key information used for encrypted communication between the first apparatus and the second apparatus in response to receiving the connection request message, and the session management apparatus sends the response message to the first apparatus via the first encrypted communication channel [0236].

As to claim 3, Birger discloses a session management apparatus for establishing an encrypted communication channel between a first apparatus and a second apparatus, the session management apparatus comprising:

a part for exchanging key information for encrypted communication with the first apparatus (i.e. The exchange of session key information.) [0211], and performing mutual authentication with the first apparatus so as to establish a first encrypted communication channel between the session management apparatus and the first apparatus (i.e. The registration process involves a mutual authentication between the endpoint and the authentication service.) [0209];

a part for exchanging key information for encrypted communication with the second apparatus, and performing mutual authentication with the second

apparatus so as to establish a second encrypted communication channel between the session management apparatus and the second apparatus (i.e. The exchange of session key information) [0214];

a part for receiving, from the first apparatus via the first encrypted communication channel, a connection request message to the second apparatus that includes key information for encrypted communication between the first apparatus and the second apparatus, and transferring the connection request message to the second apparatus via the second encrypted communication channel (i.e. Figure 9 illustrates authentication and establishing a connection) [0222-0223]; and

a part for receiving, from the second apparatus via the second encrypted communication channel, a response message that includes key information for encrypted communication between the first apparatus and the second apparatus, and transferring the response message to the first apparatus via the first encrypted communication channel [0236].

As to claim 4, Birger discloses the session management apparatus as claimed in claim 3, the session management apparatus further comprising:

a part for performing message communications between the first apparatus and the session management apparatus and between the second apparatus and the session management apparatus by using Session Initiation Protocol [0241].

As to claim 5, Birger discloses the session management apparatus as claimed in claim 3, the session management apparatus further comprising:

a part for receiving a name and an address of the first apparatus via the first encrypted communication channel, and registering the name and the address of the first apparatus in a storage device of the session management apparatus (i.e. unique identifier) [0148];

a part for receiving a name and an address of the second apparatus via the second encrypted communication channel, and registering the name and the address of the second apparatus in the storage device (i.e. unique identifier) [0148]; and

a name resolution part for obtaining the address of the second apparatus from the name of the second apparatus included in the connection request message sent from the first apparatus [0173].

As to claim 6, Birger discloses the session management apparatus as claimed in claim 3, the session management apparatus further comprising:

a part for determining whether the first apparatus is permitted to access the second apparatus by referring to access permission information stored in the session management apparatus when the session management apparatus receives the connection request message from the first apparatus, and rejecting access to the second apparatus by the first apparatus if the first apparatus is not permitted to access the second apparatus (i.e. authentication and authorization) [0088-0091].

As to claim 7, Birger discloses the session management apparatus as claimed in claim 3, the session management apparatus further comprising:

a part for receiving a public-key from the first apparatus via the first encrypted communication channel [0219-0222]; and

a part for generating a public-key certificate for the received public-key, and sending the public-key certificate to the first apparatus via the first encrypted communication channel [0219-0222].

As to claim 8, Birger discloses that the session management apparatus includes a server for establishing the first encrypted communication channel to the first apparatus, and an apparatus that is connected to the server and that generates and manages public-key certificates [0219-0222].

As to claim 9, Birger discloses the session management apparatus as claimed in claim 3, the session management apparatus further comprising:

a part for receiving a public-key of the first apparatus via the first encrypted communication channel [0219-0222];

a part for storing the received public-key in its storage device [0219-0222]; and

a part for sending the public-key of the first apparatus via the second encrypted communication channel to the second apparatus [0219-0222].

As to claim 10, Birger discloses that the session management apparatus includes a first apparatus for establishing the first encrypted communication channel and the second encrypted communication channel, and a second apparatus that is connected to the first apparatus and that manages public-keys [0219-0222].

As to claim 11, Birger discloses the session management apparatus as claimed in claim 3, the session management apparatus further comprising:

> a storage device for storing a name of the first apparatus and identification information of the first encrypted communication channel wherein the name of the first apparatus and the identification information are associated with each other (i.e. unique identifier) [0148]; and
>
> a part for determining whether a name included in the connection request message received from the first apparatus is correct by comparing the name included in the connection request message with the name that is stored in the storage device and that is associated with the identification information of the first encrypted communication channel [0173].

As to claim 12, Birger discloses that if the session management apparatus determines that the name of the first apparatus included in the connection request message is not correct, the session management apparatus sends an error message to the first apparatus [0051].

As to claim 13, Birger discloses that the connection request message received from the first apparatus includes a first header indicating reliability of a route between the first apparatus and the session management apparatus, the session management apparatus further comprising:

> a part for adding a second header indicating reliability of a route between the session management apparatus and the second apparatus to the connection request message, and sending the connection request message to the second apparatus via the second encrypted communication channel (i.e. quality of service) [0275].

As to claim 14, Birger discloses that the first header includes an address of the first apparatus, and in response to receiving the first header, the session management apparatus determines validity of the first header by comparing the address included in the first header and an address of the first apparatus (i.e. verifying addresses) [0102].

As to claim 15, Birger discloses an apparatus that establishes an encrypted communication channel to a second apparatus by using a session management apparatus, the apparatus comprising:

a part for exchanging key information for encrypted communication with the session management apparatus (i.e. The exchange of session key information.) [0211], performing mutual authentication with the session management apparatus so as to establish a first encrypted communication channel between the apparatus and the session management apparatus (i.e. The registration process involves a mutual authentication between the endpoint and the authentication service.) [0209]; and

a part for sending, to the session management apparatus via the first encrypted communication channel , a connection request message including key information for encrypted communication between the apparatus and the second apparatus, and receiving, from the second apparatus via the session management apparatus (i.e. Figure 9 illustrates authentication and establishing a connection) [0222-0223], a response message including key information for encrypted communication between the apparatus and the second apparatus so as to establish

a second encrypted communication channel between the apparatus and the second apparatus (i.e. The exchange of session key information) [0214].

As to claim 16, Birger discloses the apparatus as claimed in claim 15, wherein:

when the apparatus is accessed by a third apparatus, the apparatus establishes the first encrypted communication channel and establishes the second encrypted communication channel by using the first encrypted communication channel [0211-0214]; and

the apparatus receives data from the second apparatus via the second encrypted communication channel between the apparatus and the second apparatus, and sends the data to the third apparatus [0211-0214].

As to claim 17, Birger discloses the apparatus as claimed in claim 15, wherein:

when the apparatus is accessed by a third apparatus, the apparatus establishes the second encrypted communication channel by using the first encrypted communication channel [0211-0214]; and

the apparatus receives data from the second apparatus via the second encrypted communication channel between the apparatus and the second apparatus, and sends the data to the third apparatus [0211-0214].

As to claim 18, Birger discloses that the apparatus has a table including at least one connection destination to which the third apparatus is permitted to connect, and the apparatus sends the at least one connection destination to the third apparatus when the third apparatus accesses the apparatus, and receives a selected connection destination from the third apparatus (i.e. Figure 9 illustrates authentication and establishing a connection) [0222-0223].

As to claim 19, Birger discloses a computer program for causing a computer to function as a session management apparatus that is used for establishing an encrypted communication channel between a first apparatus and a second apparatus that are connected to a communication network, the computer program comprising:

program code means for exchanging key information for encrypted communication with the first apparatus (i.e. The exchange of session key information.) [0211], and performing mutual authentication with the first apparatus so as to establish a first encrypted communication channel between the computer and the first apparatus (i.e. The registration process involves a mutual authentication between the endpoint and the authentication service.) [0209];

program code means for exchanging key information for encrypted communication with the second apparatus, and performing mutual authentication with the second apparatus so as to establish a second encrypted communication channel between the computer and the second apparatus (i.e. The exchange of session key information) [0214];

program code means for receiving, from the first apparatus via the first encrypted communication channel, a connection request message to the second apparatus that includes key information for encrypted communication between the first apparatus and the second apparatus, and transferring the connection request message to the second apparatus via the second encrypted communication channel (i.e. Figure 9 illustrates authentication and establishing a connection) [0222-0223]; and

program code means for receiving, from the second apparatus via the second encrypted communication channel, a response message that includes key information for encrypted communication between the first apparatus and the second apparatus, and transferring the response message to the first apparatus via the first encrypted communication channel [0236].

As to claim 20, Birger discloses the computer program as claimed in claim 19, the computer program further comprising:

program code means for receiving a public-key from the first apparatus via the first encrypted communication channel [0219-0222]; and

program code means for generating a public-key certificate for the received public-key, and sending the public-key certificate to the first apparatus via the first encrypted communication channel [0219-0222].

As to claim 21, Birger discloses the computer program as claimed in claim 19, the computer program further comprising:

program code means for receiving a public-key of the first apparatus via the first encrypted communication channel [0219-0222];

program code means for storing the received public-key in a storage device [0219-0222]; and

program code means for sending the public-key of the first apparatus via the second encrypted communication channel to the second apparatus [0219-0222].

As to claim 22, Birger discloses a computer program for causing a computer to function as an apparatus that establishes an encrypted communication channel to a second apparatus by using a session management apparatus, the computer program comprising:

program code means for exchanging key information for encrypted communication with the session management apparatus (i.e. The exchange of session key information.) [0211], performing mutual authentication with the session management apparatus so as to establish a first encrypted communication channel between the computer and the session management apparatus (i.e. The registration process involves a mutual authentication between the endpoint and the authentication service.) [0209]; and

program code means for sending, to the session management apparatus via the first encrypted communication channel, a connection request message including key information for encrypted communication between the apparatus and the second apparatus (i.e. Figure 9 illustrates authentication and establishing a connection) [0222-0223], and receiving, from the second apparatus via the session management apparatus, a response message including key information for encrypted communication between the apparatus and the second apparatus so as to establish a second encrypted communication channel between the apparatus and the second apparatus (i.e. The exchange of session key information) [0214].

As to claim 23, Birger discloses the computer program as claimed in claim 19, the computer program further comprising:

program code means for storing a name of the first apparatus and identification information of the first encrypted communication channel in a storage device wherein the name of the first apparatus and the identification information are associated with each other (i.e. unique identifier) [0174]; and

program code means for determining whether a name included in the connection request message received from the first apparatus is correct by comparing the name included in the connection request message with the name that is stored in the storage device and that is associated with the identification information of the first encrypted communication channel [0250].

As to claim 24, Birger discloses that the connection request message received from the first apparatus includes a first header indicating reliability of a route between the first apparatus and the session management apparatus, the computer program further comprising:

program code means for adding a second header indicating reliability of a route between the session management apparatus and the second apparatus to the connection request message, and sending the connection request message to the second apparatus via the second encrypted communication channel (i.e. Figure 9 illustrates authentication and establishing a connection) [0222-0223].

As to claim 25, Birger discloses a method for establishing an encrypted communication channel between a first apparatus and a second apparatus, wherein:

a public-key management apparatus and the first apparatus exchange key information used for encrypted communication (i.e. The exchange of session key information.) [0211], and the public-key management apparatus and the first

apparatus perform mutual authentication so that a first encrypted communication channel is established (i.e. The registration process involves a mutual authentication between the endpoint and the authentication service.) [0209];

the first apparatus generates a secret key and a public-key, and sends the public-key to the public-key management apparatus via the first encrypted communication channel (i.e. The exchange of session key information) [0214];

the public-key management apparatus generates a public-key certificate for the received public-key, and sends the public-key certificate to the first apparatus via the first encrypted communication channel [0219]; and

the first apparatus sends the public-key certificate to the second apparatus so that a second encrypted communication channel using the public-key between the first apparatus and the second apparatus is established [0219].

As to claim 26, Birger discloses a method for establishing an encrypted communication channel between a first apparatus and a second apparatus, wherein:

a public-key management apparatus and the first apparatus exchange key information used for performing encrypted communication (i.e. The exchange of session key information.) [0211], and the public-key management apparatus and the first apparatus perform mutual authentication so that a first encrypted communication channel is established (i.e. The registration process involves a mutual authentication between the endpoint and the authentication service.) [0209];

the public-key management apparatus and the second apparatus exchange key information used for encrypted communication, and the public-key management apparatus and the second apparatus perform mutual authentication so that a second encrypted communication channel is established [0219-0222];

the first apparatus generates a secret key and a public-key, and sends the public-key to the public-key management apparatus via the first encrypted communication channel [0219-0222];

the public-key management apparatus stores the received public-key in its storage device, and the second apparatus obtains the public-key from the public-key management apparatus via the second encrypted communication channel so that a third encrypted communication channel using the public-key between the first apparatus and the second apparatus is established [0219-0222].

As to claim 27, Birger discloses a public-key management apparatus for managing public-keys used for establishing an encrypted communication channel between a first apparatus and a second apparatus, the public-key management apparatus comprising:

a part for exchanging key information for encrypted communication with the first apparatus (i.e. The exchange of session key information.) [0211], and performing mutual authentication with the first apparatus so as to establish a first encrypted communication channel (i.e. The registration process involves a mutual authentication between the endpoint and the authentication service.) [0209];

a part for receiving a public-key from the first apparatus via the first encrypted communication channel [0219-0222]; and

a part for generating a public-key certificate for the received public-key, and sending the public-key certificate to the first apparatus via the first encrypted communication channel [0219-0222].

As to claim 28, Birger discloses that the public-key management apparatus includes a server for establishing the first encrypted communication channel to the first apparatus, and an apparatus that is connected to the server and that generates and manages public-key certificates [0219-0222].

As to claim 29, Birger discloses that the public-key management apparatus further includes a part for performing message communications between the first apparatus and the public-key management apparatus by using Session Initiation Protocol [0219-0222].

As to claim 30, Birger discloses a public-key management apparatus for managing public-keys used for establishing an encrypted communication channel between a first apparatus and a second apparatus, the public-key management apparatus comprising:

a part for exchanging key information for encrypted communication with the first apparatus (i.e. The exchange of session key information.) [0211], and performing mutual authentication with the first apparatus so as to establish a first encrypted communication channel (i.e. The registration process involves a mutual authentication between the endpoint and the authentication service.) [0209];

a part for exchanging key information for encrypted communication with the second apparatus, and performing mutual authentication with the second apparatus so as to establish a second encrypted communication channel (i.e. The exchange of session key information) [0214];

a part for receiving a public-key of the first apparatus via the first encrypted communication channel [0219-0222];

a part for storing the received public-key in its storage device [0219-0222]; and

a part for sending the public-key of the first apparatus via the second encrypted communication channel to the second apparatus [0219-0222].

As to claim 31, Birger discloses that the public-key management apparatus includes a first apparatus for establishing the first encrypted communication channel and the second encrypted communication channel, and a second apparatus that is connected to the first apparatus and that manages public-keys [0219-0222].

As to claim 32, Birger discloses the public-key management apparatus as claimed in claim 30, the public-key management apparatus further comprising:

a part for performing message communications between the first apparatus and the public-key management apparatus and between the second apparatus and the public-key management apparatus by using Session Initiation Protocol [0219-0222].

As to claim 33, Birger discloses a computer program for causing a computer to function as a public-key management apparatus for managing public-keys, the computer program comprising:

program code means for exchanging key information for encrypted communication with a first apparatus (i.e. The exchange of session key information.) [0211], and performing mutual authentication with the first

apparatus so as to establish a first encrypted communication channel (i.e. The registration process involves a mutual authentication between the endpoint and the authentication service.) [0209];

program code means for receiving a public-key from the first apparatus via the first encrypted communication channel [0219-0222]; and

program code means for generating a public-key certificate for the received public-key, and sending the public-key certificate to the first apparatus via the first encrypted communication channel [0219-0222].

As to claim 34, Birger discloses a computer program for causing a computer to function as a public-key management apparatus for managing public-keys used for establishing an encrypted communication channel between a first apparatus and a second apparatus, the computer program comprising:

program code means for exchanging key information used for encrypted communication with the first apparatus (i.e. The exchange of session key information.) [0211], and performing mutual authentication with the first apparatus so as to establish a first encrypted communication channel (i.e. The registration process involves a mutual authentication between the endpoint and the authentication service.) [0209];

program code means for exchanging key information for encrypted communication with the second apparatus, and performing mutual authentication with the second apparatus so as to establish a second encrypted communication channel (i.e. The exchange of session key information) [0214];

program code means for receiving a public-key of the first apparatus via the first encrypted communication channel [0219-0222];

program code means for storing the received public-key in a storage device [0219-0222]; and

program code means for sending the public-key of the first apparatus via the second encrypted communication channel to the second apparatus [0219-0222].

As to claim 35, Birger discloses a session management apparatus that can connect to a first apparatus and a second apparatus over a network, the session management apparatus comprising:

a part for performing mutual authentication with the first apparatus to establish a first encrypted communication channel between the session management apparatus and the first apparatus (i.e. The registration process involves a mutual authentication between the endpoint and the authentication service.) [0209], and storing a name of the first apparatus and identification information of the first encrypted communication channel in a storage device wherein the name of the first apparatus and the identification information are associated with each other (i.e. unique identifier) [0174];

a part for establishing a second encrypted communication channel between the session management apparatus and the second apparatus based on mutual authentication with the second apparatus (i.e. the second phase is session management that includes conducting mutual authentication) [0216];

a part for receiving a message including a name of the first apparatus via the first encrypted communication channel (i.e. unique identifier) [0174];

a part for determining whether the name included in the message is correct by comparing the name included in the message with the name that is stored in the storage device and that is associated with the identification information of the first encrypted communication channel [0250]; and

a part for sending the message to the second apparatus via the second encrypted communication channel [0257].

As to claim 36, Birger discloses that if the session management apparatus determines that the name of the first apparatus included in the message is not correct, the session management apparatus sends an error message to the first apparatus [0051].

As to claim 37, Birger discloses a session management apparatus that can connect to a first apparatus and a second apparatus over a network, the session management apparatus comprising:

a part for performing mutual authentication with the first apparatus to establish a first encrypted communication channel between the session management apparatus and the first apparatus (i.e. The registration process involves a mutual authentication between the endpoint and the authentication service.) [0209];

a part for establishing a second encrypted communication channel between the session management apparatus and the second apparatus based on

mutual authentication with the second apparatus (i.e. the second phase is session management that includes conducting mutual authentication) [0216];

a part for receiving, from the first apparatus via the first encrypted communication channel, a message including a first header indicating reliability of a route between the first apparatus and the session management apparatus (i.e. quality of service) [0275]; and

a part for adding a second header indicating reliability of a route between the session management apparatus and the second apparatus to the message, and sending the message to the second apparatus via the second encrypted communication channel (i.e. quality of service) [0275].

As to claim 38, Birger discloses that the first header includes an address of the first apparatus, and in response to receiving the first header, the session management apparatus determines validity of the first header by comparing an address included in the first header and an address of the first apparatus (i.e. authenticating addresses) [0090].

As to claim 39, Birger discloses that the message is based on Session Initiation Protocol [0241].

As to claim 40, Birger discloses a method for transferring a message among a first apparatus, a session management apparatus and a second apparatus each connected to a network, wherein:

the session management apparatus and the first apparatus perform mutual authentication to establish a first encrypted communication channel between the session management apparatus and the first apparatus (i.e. The registration

process involves a mutual authentication between the endpoint and the authentication service.) [0209], and the session management apparatus stores a name of the first apparatus and identification information of the first encrypted communication channel in a storage device wherein the name of the first apparatus and the identification information are associated with each other (i.e. unique identifier) [0174];

the session management apparatus and the second apparatus performs mutual communication to establish a second encrypted communication channel between the session management apparatus and the second apparatus (i.e. the second phase is session management that includes conducting mutual authentication) [0216];

the first apparatus sends a message including a name of the first apparatus via the first encrypted communication channel to the session management apparatus (i.e. the unique identifier) [0174];

the session management apparatus determines whether the name included in the message is correct by comparing the name included in the message with the name that is stored in the storage device and that is associated with the identification information of the first encrypted communication channel [0250]; and

the session management apparatus sends the message to the second apparatus via the second encrypted communication channel [0257].

As to claim 41, Birger discloses a method for transferring a message among a first apparatus, a session management apparatus and a second apparatus each connected to a network, wherein:

the session management apparatus and the first apparatus perform mutual authentication to establish a first encrypted communication channel between the session management apparatus and the first apparatus (i.e. The registration process involves a mutual authentication between the endpoint and the authentication service.) [0209];

the session management apparatus and the second apparatus perform mutual communication to establish a second encrypted communication channel between the session management apparatus and the second apparatus (i.e. the second phase is session management that includes conducting mutual authentication) [0216];

the first apparatus sends, to the session management apparatus via the first encrypted communication channel, a message including a first header indicating reliability of a route between the first apparatus and the session management apparatus (i.e. quality of service) [0275]; and

the session management apparatus adds a second header indicating reliability of a route between the session management apparatus and the second apparatus to the message, and sends the message to the second apparatus via the second encrypted communication channel (i.e. quality of service) [0275].

As to claim 42, Birger discloses a computer program for causing a computer to function as a session management apparatus that can connect to a first apparatus and a second apparatus over a network, the computer program comprising:

program code means for performing mutual authentication with the first apparatus to establish a first encrypted communication channel between the session management apparatus and the first apparatus (i.e. The registration process involves a mutual authentication between the endpoint and the authentication service.) [0209], and storing a name of the first apparatus and identification information of the first encrypted communication channel in a storage device wherein the name of the first apparatus and the identification information are associated with each other (i.e. unique identifier) [0174];

program code means for establishing a second encrypted communication channel between the session management apparatus and the second apparatus based on mutual authentication with the second apparatus (i.e. the second phase is session management that includes conducting mutual authentication) [0216];

program code means for receiving a message including a name of the first apparatus via the first encrypted communication channel (i.e. unique identifier) [0174];

program code means for determining whether the name included in the message is correct by comparing the name included in the message with the name that is stored in the storage device and that is associated with the identification information of the first encrypted communication channel [0250]; and

program code means for sending the message to the second apparatus via the second encrypted communication channel [0257].

As to claim 43, Birger discloses a computer program for causing a computer to function as a session management apparatus that can connect to a first apparatus and a second apparatus over a network, the computer program comprising:

program code means for performing mutual authentication with the first apparatus to establish a first encrypted communication channel between the session management apparatus and the first apparatus (i.e. The registration process involves a mutual authentication between the endpoint and the authentication service.) [0209];

program code means for establishing a second encrypted communication channel between the session management apparatus and the second apparatus based on mutual authentication with the second apparatus (i.e. the second phase is session management that includes conducting mutual authentication) [0216];

program code means for receiving, from the first apparatus via the first encrypted communication channel, a message including a first header indicating reliability of a route between the first apparatus and the session management apparatus (i.e. quality of service) [0275]; and

program code means for adding a second header indicating reliability of a route between the session management apparatus and the second apparatus to the message, and sending the message to the second apparatus via the second encrypted communication channel (i.e. quality of service) [0275].

Conclusion

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K. Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Aravind K Moorthy/
Examiner, Art Unit 2431